Amendments to the Drawings

The attached sheet of drawings includes the Figure on a separate sheet. The sheet replaces the original sheet including the Figure.

Attachment: 1 Replacement Sheet

REMARKS

Claim 1 has been canceled and claims 2-21 have been added. Support for these claims may be found through the specification. No new matter has been entered.

Specification

The specification has been amended to provide minor corrections to spelling and grammar throughout the specification. A substitute specification with the proposed changes is attached hereto along with a marked-up copy of the published application indicating the changes. No new matter has been added by these changes. Entry of the proposed substitute specification is requested.

Drawing

A drawing on a separate page has been provided to replace the informal drawing of record. No new matter has been entered.

Claim Rejections - 35 U.S.C. §§112 and 102(e)

Claim 1 stands rejected under 35 U.S.C. §112, second paragraph, as allegedly being indefinite as being directed to a system and a method. Also, claim 1 stands rejected under 35 U.S.C. §102(e) as allegedly being anticipated by McClure et al. (US 7,152,105). Applicant has canceled claim 1, thereby obviating these rejections. Withdrawal of all rejections of claim 1 is solicited.

New claims 2-21

New claims 2-21 are believed to satisfy the requirements of 35 U.S.C. §112 and to clearly distinguish over the teachings of McClure et al. The Examiner is asked to note that McClure et al. do not contemplate a method or system that provides "at least one agent disposed in said computer network to passively collect, monitor, and aggregate data representative of activities of respective nodes within said computer network," or that analyzes the collected data "to develop activity models representative of activities of said network in a normal state and activities of said network in an abnormal state." McClure et al. also do not disclose a method or system that compares the collected data to the activity models "to determine the state of said computer network at different times and to dynamically update said activity models" as claimed. The claimed method "passively" collects the network data by sampling the data traffic, not by transmitting data packets to a

target computer to get a response for analysis. McClure et al. actively probes the nodes in the computer network by sending data packets and analyzing the responses to determine the operating system of the target node. In contrast, the claimed system and method passively monitors the activity to identify patterns representative of suspicious network activity. Such a system and method is not taught by McClure et al. Allowance of claims 2-21 over McClure et al. is thus believed to be proper and is respectfully solicited.

Conclusion

In view of the above, the present application is believed to be in condition for allowance and a Notice to that effect is respectfully solicited.

Date: Monday, September 17, 2007

/Michael P. Dunnam/
Michael P. Dunnam
Registration No. 32,611

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439